UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/619,031	07/14/2003	Alain Chatcau	TI-34920	6390

23494 7590 12/12/2006

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/619,031	CHATEAU ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-17 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-17 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 14 July 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 12/01/03.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 have been examined.

Claim Objections

2. Claim 2 is objected to because of the following informalities: "wherein digital certificate comprises contains" (line 2) should be changed to "wherein the digital certificate contains". Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 4 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 4, which depends from claim 2, recites the limitation "wherein the signature further contains a signature for selected fields of the digital certificate". The signature of claim 2 is a software signature; however, the specification does not disclose that the software signature is a signature for certain fields of the

certificate. According to the specification, it is the certificate signature which is a signature for certain fields of the certificate. For examination purpose, the limitation is interpreted as "wherein the digital certificate further contains a signature for selected fields of the digital certificate".

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 7-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 7 recites the limitation "the electronic file" in 8. There is insufficient antecedent basis for this limitation in the claim.

7. Claims 1-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 1 fails to interrelate essential elements of the claimed invention as defined by Applicant in the specification. Claim 1 recites the following elements: (1) a random key associated with (2) a selected electronic file to be stored, and (3) a certificate containing an encrypted form of the random key such that the file can be accessed only after the encrypted random key

is decrypted. However, the claim fails to recite the interrelationship between the elements as defined in the specification: the key is used to sign the file certificate, the file is encrypted using the key, the file cannot be accessed until the file certificate is verified using the key and the encrypted file is decrypted using the key (figures 10-11 and corresponding text). Claim 7 is rejected on the same basis as claim 1. Claims that are not specifically addressed are rejected by virtue of their dependency.

- Claim 2 recites "a software signature" (line 2). However, there is no software recited in either claim 2 or independent claim 1; and claim 2 fails to recite the interrelationship between the software signature and other elements of the claim as defined by Applicant in the specification: the software signature being a signature for the electronic file that is symmetrically encrypted using the random key (fig. 10). Claim 8 is rejected on the same basis as claim 2.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claim 16 is rejected under 35 U.S.C. 102(b) as being anticipated by Ehrsam et al. (4,238,854). Ehrsam discloses a method of storing a protected file in an externally-accessible memory of a host system which includes a data security device (Abstract; figures 1-2) comprising: storing a secret identification number (i.e., a secure host master key) for the host system in a secure memory of the data security device that is not externally-accessible; generating a random key (i.e., an operational key) associated with a selected electronic file to be stored in the externally-accessible memory; generating an encoded key by symmetrically encrypting the random key using the secret identification number and a key encrypting key (i.e., a file key); encrypting the selected electronic file using the random key and storing the encrypted electronic file in the externally-accessible memory; and storing the encrypted key in the externally-accessible memory and associating the encrypted key with the encrypted electronic file (i.e., storing the encrypted key in the file header of the encrypted electronic file), such that the encrypted electronic file can be decrypted only after restoring the random key through decryption of the encrypted key with the secret identification number (figure 15; col. 20, line 54 – col. 22, line 35).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 5-7 and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ehrsam in view of Pham et al. (6,931,530). Regarding claims 7 and 11-13, which are representative of claims 1 and 5-6, Ehrsam discloses a method of storing a protected file in an externally-accessible memory of a host system which includes a data security device (Abstract; figures 1-2) comprising: storing a secret identification number (i.e., a secure host master key) for the host system in a secure memory of the data security device that is not externally-accessible; generating a random key (i.e., an operational key) associated with a selected electronic file to be stored in the externally-accessible memory; generating an encoded key by symmetrically encrypting the random key using the secret identification number and a key encrypting key (i.e., a file key); encrypting the selected electronic file using the random key and storing the encrypted electronic file in the externally-accessible memory; and storing the encrypted key in the file header of the encrypted electronic file in the externally-accessible

memory, such that the encrypted electronic file can be decrypted only after restoring the random key through decryption of the encrypted key with the secret identification number (figure 15; col. 20, line 54 – col. 22, line 35). Ehrsam does not disclose singing the file header. Pham discloses signing a file header containing information related to an encrypted file including key information for decrypting the encrypted file, and including the signature as part of the file header (figure 8C, element 226; figure 8D, elements 228-238; col. 16, table 1; col. 17, lines 24-33). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the Ehrsam method to sign the file header, as taught by Pham. The motivation for doing so would have been to enable detection of tampering with the file header. Such a file header meets the limitation of the certificate of the claimed invention.

12. Claims 2-4, 8-10 and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ehrsam in view of Pham as applied to claims 1 and 7 above, and further in view of Ellison et al. (7,082,615).

Regarding claims 2-3, 8-9 and 14-15, Pham discloses storing various other information related to a file in the file header (col. 17, lines 20-23). Ehrsam and Pham do not disclose such information is the file signature, i.e., hash value of the file symmetrically encrypted using the file encryption key

(i.e., the random key). Ellison discloses file related information being the signature of a file generated by hashing the file and symmetrically encrypting the hash value using a file encryption key (figure 3B; col. 10, lines 31-62). It would have been obvious to one of ordinary in the art at the time the invention was made to modify the combined method Ehrsam and Pham such that file related information is the file signature, as taught by Ellison. The motivation for doing so would have been to enable detection of unauthorized modification of the file.

Regarding claims 4 and 10, Pham further discloses that the header signature is a signature for selected parts of the header (col. 16, lines 63-65).

13. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ehrsam as applied to claim 16 above, and further in view of Ellison. Ehrsam does not disclose storing an encrypted software signature for the electronic file in the externally-accessible memory, where the software signature is a hash of the electronic file, encrypted using the random key. Ellison discloses storing an encrypted signature for a electronic file in externally-accessible memory, where the software signature is a hash of the electronic file, encrypted using a file encryption key (figure 3B; col. 10, lines 31-62). It would have been obvious to one of ordinary in the art at the time

the invention was made to modify the Ehrsam method to store an encrypted software signature for the electronic file in the externally-accessible memory, where the software signature is a hash of the electronic file, encrypted using the file encryption key, as taught by Ellison. The motivation for doing so would have been to enable detection of unauthorized modification of the file.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,416,840 to Cane et al.

U.S. Patent No. 6,014,745 to Ashe

U.S. Patent No. 5,958,051 to Renaud et al.

U.S. Patent No. 7,055,175 to Le Pennec et al.

U.S. Patent No. 7,114,082 to Klein

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

MD
12/02/06

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100